Fault detection for discrete event systems using Petri nets with unobservable transitions

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu
Dip. di Ing. Elettrica ed Elettronica, Università di Cagliari, Italy
Email: {cabasino,giua,seatzu}@diee.unica.it

Abstract

In this paper we present a fault detection approach for discrete event systems using Petri nets. We assume that some of the transitions of the net are unobservable, including all those transitions that model faulty behaviors. Our diagnosis approach is based on the notions of basis marking and justification, that allow us to characterize the set of markings that are consistent with the actual observation, and the set of unobservable transitions whose firing enable it. This approach applies to all net systems whose unobservable subnet is acyclic. If the net system is also bounded the proposed approach may be significantly simplified by moving the most burdensome part of the procedure off-line, thanks to the construction of a graph, called the *basis reachability graph*.

Published as: M.P. Cabasino, A. Giua, C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, Vol. 46, No. 9, pp. 1531-1539, September 2010.

This work has been partially supported by the European CommunityŠs Seventh Framework Programme under project DISC (Grant Agreement n. INFSO-ICT-224498).

1 Introduction

The diagnosis of discrete event systems is a research area that has received a lot of attention in the last years and has been motivated by the practical need of ensuring the correct and safe functioning of large complex systems. In the context of automata Sampath *et al.* [15, 16] propose an approach to failure diagnosis where the system is modeled as a nondeterministic automaton in which the failures are treated as unobservable events. In [15] they provide a definition of diagnosability in the framework of formal languages and establish necessary and sufficient conditions for diagnosability. Moreover, in [14] Sampath *et al.* present an integrated approach to control and diagnosis. More specifically, the authors present an approach for the design of diagnosable systems by appropriate design of the system controller and this approach is called active diagnosis. They formulate the active diagnosis problem as a supervisory control problem. In [7] Debouk *et al.* propose a coordinated decentralized architecture consisting of two local sites communicating with a coordinator that is responsible for diagnosing the failures occurring in the system. In [4] Boel and van Schuppen address the problem of synthesizing communication protocols and failure diagnosis algorithms for decentralized failure diagnosis of DES with costly communication between diagnosers. In [17] a state-based approach for on-line passive fault diagnosis is presented.

More recently, Petri net models have been used in the context of diagnosis due to their intrinsically distributed nature where the notions of state (i.e., marking) and action (i.e., transition) are local. This has often been an asset to reduce the computational complexity involved in solving a diagnosis problem. Among the first pioneering works dealing with Petri nets (PNs), we recall the approach of Prock that proposes an on-line technique for fault detection that is based on monitoring the number of tokens residing into P-invariants [13]. In [9] Genc and Lafortune propose a diagnoser on the basis of a modular approach that performs the diagnosis of faults in each module. In [2] Benveniste *et al.* present a net unfolding approach for designing an on-line asynchronous diagnoser. In [1] Basile *et al.* present a diagnosis approach where the diagnoser is built on-line by defining and solving integer linear programming problems. In [8], in order to avoid the redesign and the redefinition of the diagnoser when the structure of the system changes, Dotoli *et al.* propose a diagnoser that works on-line.

The main difference between the diagnosis approach presented here and the approaches cited above is the concept of basis marking. This concept allows us to represent the reachability space in a compact manner, i.e., our approach requires to enumerate only a subset of the reachability space. More specifically, in this paper we deal with the failure diagnosis of discrete event systems modeled by place/transition nets. We assume that faults are modeled by unobservable transitions, but there may also exist other transitions that represent legal behaviors and are unobservable as well. Thus we assume that the set of transitions can be partitioned as $T = T_o \cup T_u$ where T_o is the set of observable transitions, and T_u is the set of unobservable transitions. The set of fault transitions is denoted T_f and satisfies $T_f \subseteq T_u$.

The set of fault transitions is further partitioned into r subsets, T_f^i, $i = 1, \ldots, r$, each one corresponding to a fault class. We are not interested in distinguishing among transitions within the same class, but we want to detect the class of faults that has occurred, or that may have

occurred, given the observed behavior, i.e., the sequence of transitions that has been observed.

We associate two different sets to any observed word w, i.e., to any sequence of observed transitions:

• $\mathcal{L}(w)$ is the set containing all sequences of transitions that are consistent with w, i.e., the set of all possible firing sequences that produce observation w.

• $\mathcal{J}(w)$ is the set of *justifications*, i.e., the set of all *minimal* sequences of unobservable transitions (namely those sequences of unobservable transitions whose firing vector is minimal) interleaved with w and whose firing enables w[1].

Note, in fact, that even if a word $w \in T_o^*$ is observed, in general the sequence $\sigma = w$ is not firable on the net, i.e., it cannot occur at the initial marking: it is necessary to interleave it with a sequence σ_u of unobservable events to obtain a firable sequence σ that produces the observed word w. $\mathcal{J}(w)$ is the set of all sequences σ_u that are minimal, i.e., that have a minimal firing vector.

Now, given a fault class T_f^i and an observation w, we distinguish the following four cases, each one corresponding to an increasing level of alarm (the diagnosis state varies from 0 to 3).

(0) No sequence in $\mathcal{L}(w)$ contains a transition in T_f^i, thus no fault in the ith class has occurred.

(1) Some transitions in T_f^i may have fired but none of them was contained in a justification of w.

(2) Some transitions in T_f^i may have fired and are contained in some of the justifications of w. However, not all justifications of w contain transitions in T_f^i.

(3) All justifications of w contain transitions in T_f^i, thus a fault must have occurred.

We provide a fault detection procedure that enables us to evaluate, for any observed word and any fault class, the corresponding diagnosis state. This procedure may be carried out by simply performing matrix multiplications and evaluating the feasibility of certain integer constraint sets. Such a procedure may be applied to all net systems whose unobservable subnet is acyclic. This assumption, that is analogous to the classical hypothesis in the theory of automata where no cycle of unobservable events can appear, allows us to: (a) study the reachability of the unobservable subnet with the state equation; (b) give an easy algorithm for the computation of the firing vectors relative to justifications. In particular, (a) implies that we can distinguish between the diagnosis states 0 and 1 in an efficient way.

The most burdensome part of the proposed procedure consists in evaluating the feasibility of a finite number of integer constraint sets. We show that in the case of bounded net systems this computation may be performed off-line. An oriented graph, that we call *basis reachability graph* (BRG) may be constructed, that summarizes all the information required for diagnosis. Therefore, given any observable word w, for any fault class T_f^i we may evaluate the corresponding

[1] A sequence $\sigma \in T_u^*$ interleaved with w and enabling w is *minimal* if $\nexists \sigma' \in T_u^*$ interleaved with w and enabling w such that $\pi(\sigma') \lneq \pi(\sigma)$, where $\pi(\sigma)(\pi(\sigma'))$ denotes the firing vector associated with $\sigma(\sigma')$.

diagnosis state, by simply looking at the BRG.

This paper builds on our previous results in [6] where an observer for nets with silent transitions was designed under two structural assumptions, namely the unobservable subnet is *acyclic* and *backward conflict-free*. In such a case the set of markings that are consistent with the actual observation $\mathcal{C}(w)$, namely the set of markings that can be reached from the initial marking firing the observed word w interleaved with sequences of unobservable transitions that enable w, may be characterized by a finite set of linear algebraic constraints whose structure is *fixed*, and does not depend on the length of the observed word w. In this paper we show that a finite linear algebraic characterization of the set $\mathcal{C}(w)$ may still be given, but the number of constraints is not fixed and depends in general on the word w. This requires a generalization of the notion of basis marking with respect to [6]. In particular, here we extend this notion to arbitrary nets. This makes a completely different characterization necessary in terms of new original notions such as *justifications, minimal explanations*. Moreover, no mention of the diagnosis problem was done in [6].

2 Petri nets: main definitions

Petri nets are a family of models. In this paper we deal with the basic purely logic model called Place/Transition nets or P/T nets.

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of places; T is a set of transitions; $Pre : P \times T \rightarrow \mathbb{N}$ and $Post : P \times T \rightarrow \mathbb{N}$ are the *pre–* and *post–* incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix. We denote as $m = |P|$ and $n = |T|$ the cardinality of the set of places and transitions.

A *marking* is a vector $M : P \rightarrow \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer number of tokens, represented by black dots. We denote $M(p)$ the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0.

A transition t is enabled at M iff $M \geq Pre(\cdot\,, t)$ and may fire yielding the marking $M' = M + C(\cdot\,, t)$. We write $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. We also write $t \in \sigma$ to denote that a transition t is contained in σ.

The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \ \mid \ M_0[\sigma\rangle\}$.

Given a sequence $\sigma \in T^*$, we call $\pi : T^* \rightarrow \mathbb{N}^n$ the function that associates to σ a vector $y = \pi(\sigma) \in \mathbb{N}^n$, named the *firing vector* of σ, where $y(t) = k$ if transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted $R(N, M_0)$. Finally, we denote $PR(N, M_0)$ the *potentially reachable set*, i.e., the set of all markings

$M \in \mathbb{N}^m$ for which there exists a vector $y \in \mathbb{N}^n$ that satisfies the *state equation* $M = M_0 + C \cdot y$, i.e., $PR(N, M_0) = \{M \in \mathbb{N}^m \mid \exists\, y \in \mathbb{N}^n : M = M_0 + C \cdot y\}$. It holds that $R(N, M_0) \subseteq PR(N, M_0)$.

A PN having no oriented cycle is called *acyclic*.

Theorem 2.1 *[6] Let N be an acyclic Petri net.*
(i) If the vector $y \in \mathbb{N}^n$ satisfies the equation $M_0 + C \cdot y \geq \vec{0}$ there exists a firing sequence σ firable from M_0 whose firing vector is $\pi(\sigma) = y$.
(ii) A marking M is reachable from M_0 iff there exists a nonnegative integer solution y satisfying the state equation $M = M_0 + C \cdot y$, i.e., $R(N, M_0) = PR(N, M_0)$.

Note that in Theorem 2.1 obviously (i) implies (ii). Moreover, given a vector $y \in \mathbb{N}^n$ defined as in (i), the problem of determining a sequence with firing vector y that is enabled at M_0 may be computationally demanding and its complexity highly increases with n and with $\sum_{t \in T} y(t)$.

A net system $\langle N, M_0 \rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$. A net is said *structurally bounded* if it is bounded for any initial marking.

A P/T net is *backward conflict-free* if each place $p \in P$ has at most one input transition.

We assume that the set of transitions T is partitioned in two subsets T_o and T_u, i.e., $T = T_o \cup T_u$ and $T_o \cap T_u = \emptyset$. The set T_o includes all transitions that are *observable*, while T_u includes *unobservable* or *silent* transitions.

We denote as n_o (n_u) the cardinality of set T_o (T_u), and as C_o (C_u) the restriction of the incidence matrix to T_o (T_u).

Definition 2.2 Let $N = (P, T, Pre, Post)$ be a net with $T = T_o \cup T_u$. We define the following two operators.
— The *projection over* T_o is $P_o : T^* \to T_o^*$ defined as: (i) $P_o(\epsilon) = \epsilon$; (ii) for all $\sigma \in T^*$ and $t \in T$, $P_o(\sigma t) = P_o(\sigma)t$ if $t \in T_o$, and $P_o(\sigma t) = P_o(\sigma)$ otherwise.
— The *projection over* T_u is $P_u : T^* \to T_u^*$ defined as: (i) $P_u(\epsilon) = \epsilon$; (ii) for all $\sigma \in T^*$ and $t \in T$, $P_u(\sigma t) = P_u(\sigma)t$ if $t \in T_u$, and $P_u(\sigma t) = P_u(\sigma)$ otherwise. ■

Given a sequence $\sigma \in L(N, M_0)$, we denote $w = P_o(\sigma)$ the corresponding *observed word*.

Definition 2.3 Let $\langle N, M_0 \rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in T_o^*$ be an observed word. We define $\mathcal{L}(w) = P_o^{-1}(w) \cap L(N, M_0) = \{\sigma \in L(N, M_0) \mid P_o(\sigma) = w\}$, the set of firing sequences *consistent* with $w \in T_o^*$. ■

Definition 2.4 Let $\langle N, M_0 \rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in T_o^*$ be an observed word. We define $\mathcal{C}(w) = \{M \in R(N, M_0) \mid \exists \sigma \in \mathcal{L}(w) : M_0[\sigma\rangle M\}$, the set of markings *consistent* with $w \in T_o^*$. ■

In plain words, given an observation w, $\mathcal{L}(w)$ is the set of sequences that may have fired, while $\mathcal{C}(w)$ is the set of markings in which the system may actually be.

Example 2.5 Let us consider the net system in Fig. 1. It represents a production line processing

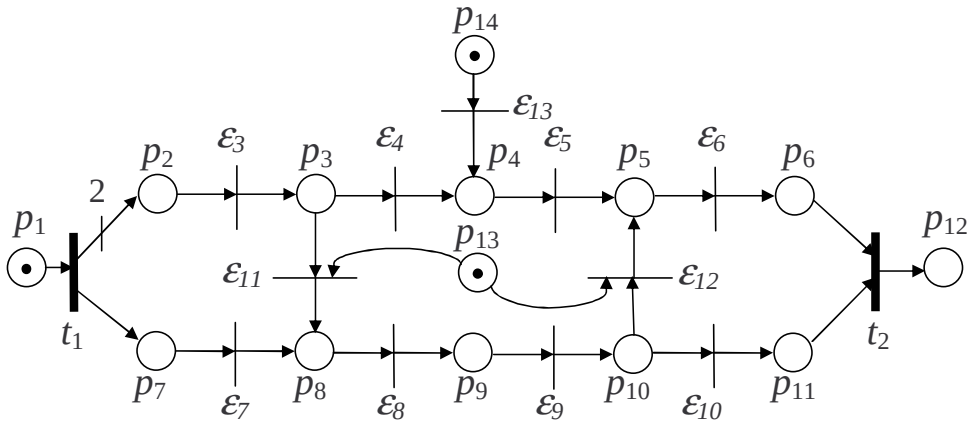

Figure 1: A PN modeling a part of a production line.

damaged parts, namely metallic slabs where two plates instead of one, have been placed in a wrong decentralized position. When a damaged part is ready to be processed (tokens in p_1) slabs and plates are separated (transition t_1) and the two plates are sent in the upper line (modeled by places p_2, p_3, p_4, p_5, p_6), while the slab is sent in the lower line (modeled by places p_7, p_8, p_9, p_{10}, p_{11}). In the two lines parts are processed, namely smoothed, cleaned up, painted and polished (this corresponds to the firing of transitions ε_3 to ε_{10}). Finally one metallic plate is inserted in the slab in the correct position (transition t_2). The second plate is used again for other slabs, but this part of the process is not modeled here.

We assume that $T_o = \{t_1, t_2\}$ and $T_u = \{\varepsilon_3, \varepsilon_4, \ldots, \varepsilon_{13}\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i.

Assume no event is observed, namely $w = \varepsilon$. It holds that $\mathcal{L}(\varepsilon) = \{\varepsilon, \varepsilon_{13}, \varepsilon_{13}\varepsilon_5, \varepsilon_{13}\varepsilon_5\varepsilon_6\}$ and $\mathcal{C}(\varepsilon) = \{M_0, M_1, M_2, M_3\}$, where M_0 is the initial marking, $M_1 = [1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$, $M_2 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$ and $M_3 = [1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$.

Now, assume t_1 is observed. Transition t_1 is enabled at the initial marking, thus the firing of no unobservable transition is necessary to enable it. After the firing of t_1 several sequences of unobservable transitions are enabled, and several markings are thus consistent with the actual behavior. In particular, all sequences $t_1\varepsilon_3$, $t_1\varepsilon_3\varepsilon_3$, $t_1\varepsilon_3\varepsilon_3\varepsilon_4$, $t_1\varepsilon_3\varepsilon_3\varepsilon_4\varepsilon_4\varepsilon_{13}$, …, $t_1\varepsilon_7$, $t_1\varepsilon_7\varepsilon_8$, …, etc. may have fired given the actual observation, and $\mathcal{C}(w)$ includes all markings that are reached firing the above sequences.

Now, let us consider $w = t_2$. In such a case no sequence of unobservable transitions may enable it. Therefore, $\mathcal{C}(t_2) = \mathcal{L}(t_2) = \emptyset$.

Finally, let us consider $w = t_1t_2$. In such a case we obtain $\mathcal{L}(t_1t_2) = \{t_1\varepsilon_3\varepsilon_4\varepsilon_5\varepsilon_6\varepsilon_7\varepsilon_8\varepsilon_9\varepsilon_{10}t_2, \varepsilon_{13}t_1\varepsilon_3\varepsilon_4$ $\varepsilon_5\varepsilon_6\varepsilon_5\varepsilon_6\varepsilon_7\varepsilon_8\varepsilon_9\varepsilon_{10}t_2, t_1\varepsilon_3\varepsilon_{11}\varepsilon_8\varepsilon_9\varepsilon_{10}\varepsilon_{13}\varepsilon_5\varepsilon_6t_2, \varepsilon_{13}t_1\varepsilon_3\varepsilon_7\ \varepsilon_8\varepsilon_9\varepsilon_{10}\varepsilon_5\varepsilon_6, \ldots\}$, and

$$\begin{aligned}\mathcal{C}(t_1t_2) \;=\; &\big\{[0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1]^T,\\ &[0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T,\\ &[0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T,\\ &[0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T, \ldots\big\},\end{aligned}$$

where dots denote all other sequences that may have fired and all other markings consistent with t_1t_2, respectively (that have not been reported here for the sake of conciseness). ■

Definition 2.6 Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, we define the $T'-$*induced subnet of* N as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restriction of $Pre, Post$ to T'. The net N' can be thought of as obtained from N by removing all transitions in $T \setminus T'$. We also write $N' \prec_{T'} N$. ■

3 Basis markings and j-vectors

Let us first introduce some basic definitions that will be useful in the following.

Definition 3.1 Given a marking M and an observable transition $t \in T_o$, we define

$$\Sigma(M, t) = \{\sigma \in T_u^* \mid M[\sigma\rangle M',\ M' \geq Pre(\cdot, t)\}$$

the set of *explanations* of t at M, and we define $Y(M, t) = \pi(\Sigma(M, t))$ the *e-vectors* (or *explanation vectors*), i.e., firing vectors associated to the explanations. ■

Thus $\Sigma(M, t)$ is the set of unobservable sequences whose firing at M enables t.

Among the above sequences we want to select those whose firing vector is minimal. The firing vector of these sequences are called *minimal e-vectors*.

Definition 3.2 Given a marking M and a transition $t \in T_o$, we define

$$\Sigma_{\min}(M, t) = \{\sigma \in \Sigma(M, t) \mid \nexists\ \sigma' \in \Sigma(M, t) : \pi(\sigma') \lneqq \pi(\sigma)\}$$

the set of *minimal explanations* of t at M, and we define $Y_{\min}(M, t) = \pi(\Sigma_{\min}(M, t))$ the corresponding set of *minimal e-vectors*. ■

Similar definitions have also been given in [3, 11].

Theorem 3.3 *[6] Let $N = (P, T, Pre, Post)$ be a PN with $T = T_o \cup T_u$. If the T_u-induced subnet is acyclic and backward conflict-free, then $|Y_{\min}(M, t)| = 1$.*

An intuitive explanation to the above result can be given considering that the acyclicity assumption is necessary to identify the set of reachable markings using the state equation of the net. Finally, the backward conflict-freeness assumption implies that all places have at most one input unobservable transition. Thus, if some tokens are necessary in a given place to enable the firing of a given output transition, we can reconstruct how many times its single input unobservable transition has fired. On the contrary, if a place has more than one input unobservable transition, in general the enabling of an output transition may be the consequence of several minimal explanations.

Different approaches can be used to compute $Y_{\min}(M,t)$, e.g., see [3, 11]. In [10, 5] we also suggested an approach to find all vectors in $Y_{\min}(M,t)$ if applied to nets whose T_u-induced subnet is acyclic. It simply requires algebraic manipulations, and is inspired by the procedure proposed by Martinez and Silva [12] for the computation of minimal P-invariants.

Now, we introduce two of the most important concepts for our approach: *basis markings* and *j-vectors*. A basis marking M_b is a marking reached from the initial marking M_0 with the firing of the observed word w and of all unobservable transitions whose firing is necessary to enable w. A j-vector $y \in Y_{\min}(M_0, w)$ is a firing vector of unobservable transitions whose firing is necessary to reach M_b.

Definition 3.4 Let $\langle N, M_0\rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $\sigma \in L(N, M_0)$ be a firable sequence and $w = P_o(\sigma)$ the corresponding observed word. We define the set of *justifications of* w as

$$\begin{aligned}\mathcal{J}(w) = \{\sigma_u \in T_u^* \mid\ & [\exists \sigma \in \mathcal{L}(w)\ : \sigma_u = P_u(\sigma)] \wedge \\ & [\nexists \sigma' \in \mathcal{L}(w) :\ \sigma'_u = P_u(\sigma') \wedge \\ & \pi(\sigma'_u) \lneq \pi(\sigma_u)]\}\end{aligned}$$

or, more shortly, $\mathcal{J}(w)$ are minimal elements of $P_{uo} \circ P_o^{-1}(w)$ for the partial order defined by π.

Moreover, we define $Y_{\min}(M_0, w) = \{y \in \mathbb{N}^{n_u} \mid \exists \sigma_u \in \mathcal{J}(w) : \pi(\sigma_u) = y\}$ the corresponding set of *j-vectors*. ■

In simple words, $\mathcal{J}(w)$ is the set of sequences of unobservable transitions interleaved with w whose firing enables w and whose firing vector is minimal. The firing vectors of these sequences are called j-vectors.

Definition 3.5 Let $\langle N, M_0\rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let w be a given observation and $\sigma_u \in \mathcal{J}(w)$ be one of its minimal justifications. The marking $M_b = M_0 + C_u \cdot y + C_o \cdot y'$, where $y = \pi(\sigma_u)$, $y' = \pi(w)$, i.e., the marking reached firing w interleaved with the minimal justification σ_u, is called *basis marking* and y is called its *j-vector* (or *justification-vector*). ■

Obviously, because in general more than one justification may exist for a word w (the set $\mathcal{J}(w)$ is generally not a singleton), the basis marking may be not unique as well. Furthermore, two or more j-vectors may correspond to the same basis marking.

Note however that under appropriate assumptions on the T_u-induced subnet, the uniqueness of M_b may be ensured. In particular, in [6] we proved that this is true if the T_u-induced subnet is acyclic and backward conflict-free.

Definition 3.6 Let $\langle N, M_0\rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in T_o^*$ be an observed word. We define

$$\begin{aligned}\mathcal{M}(w) = \{(M, y)\ \mid\ & \exists \sigma \in \mathcal{L}(w)\ :\ M_0[\sigma\rangle M\ \wedge \\ & \sigma_u \in \mathcal{J}(w)\ :\ \sigma_u = P_u(\sigma), \\ & y = \pi(\sigma_u)\}\end{aligned}$$

the set of couples (basis marking - relative j-vector) that are *consistent* with $w \in T_o^*$. ■

Note that the set $\mathcal{M}(w)$ does not take into account the sequences of unobservable transitions that may have actually fired. It only keeps track of the basis markings that can be reached and of the firing vectors of the sequences of unobservable transitions that have fired to reach them. Indeed this is the information really significant when performing diagnosis.

Let us now introduce the following result that will be useful in the rest of the paper.

Definition 3.7 Let $\langle N, M_0 \rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in T_o^*$ be an observed word. We denote

$$\mathcal{M}_{basis}(w) = \{M \in \mathbb{N}^m \mid \quad \exists\, y \ \in \mathbb{N}^{n_u} \ \text{ and } (M, y) \in \mathcal{M}(w)\}$$

the set of basis markings at w. Moreover, we denote as $\mathcal{M}_{basis} = \bigcup_{w \in T_o^*} \mathcal{M}_{basis}(w)$ the set of all basis markings for any observation w. ■

Obviously, if the net system is bounded, then the set $\mathcal{M}_{basis}$ is finite.

We now show that our approach based on basis markings is able to characterize completely the reachability set under partial observation.

We start with a result that characterizes the firing sequences. In the following theorem we show that a sequence $\tilde{\sigma}$ is consistent with observation w if and only if there exists an equivalent sequence (i.e., a sequence with the same firing vector) that is the concatenation of two subsequences: the first one reaches a basis marking in $\mathcal{M}(w)$ and the second one contains only unobservable transitions.

Theorem 3.8 *Let us consider a net system $\langle N, M_0 \rangle$ whose unobservable subnet is acyclic. There exists a sequence $\tilde{\sigma} \in T^*$ such that $M_0[\tilde{\sigma}\rangle \tilde{M}$ with observable projection $P_o(\tilde{\sigma}) = w$ and firing vector $\pi(\tilde{\sigma}) = \tilde{y}$* if and only if *there also exists a couple $(M, y) \in \mathcal{M}(w)$ and an unobservable sequence $\sigma'' \in T_u^*$ such that $M[\sigma''\rangle \tilde{M}$ and $\tilde{y} = \pi(w) + y + \pi(\sigma'')$.*

Proof: We prove this result by induction on the length of the observed string w.

(Basis step) For $w = \varepsilon$ the result is obviously true.

(Inductive step) Assume the result is valid for v. We prove it is also true for $w = vt$ where $t \in T_o$.

(Only if). In fact, if there exists a sequence $\tilde{\sigma} \in T^*$ such that $M_0[\tilde{\sigma}\rangle \tilde{M}$ with $P_o(\tilde{\sigma}) = w$ and $\pi(\tilde{\sigma}) = \tilde{y}$ then there exist sequences σ' and σ'' such that

$$M_0[\sigma'\rangle M'[t\rangle M''[\sigma''\rangle \tilde{M}$$

where $P_o(\sigma') = v$, and $\sigma'' \in T_u^*$. By induction, there exists $(M, y) \in \mathcal{M}(v)$ such that

$$M_0[\sigma'_a\rangle M[\sigma'_b\rangle M'[t\rangle M''[\sigma''\rangle \tilde{M} \tag{1}$$

where $P_o(\sigma'_a) = v$, $\pi(\sigma'_a) = \pi(v) + y$ and $\sigma'_b \in T_u^*$.

By definition of minimal explanation, there exists a sequence $\sigma'_c \in \Sigma_{\min}(M,t)$ such that

$$M[\sigma'_c\rangle M'_c[t\rangle M'_d \tag{2}$$

with $\pi(\sigma'_c) \leq \pi(\sigma'_b)$ and $(M'_c, \pi(\sigma'_c)) \in \mathcal{M}(vt) = \mathcal{M}(w)$.

We now claim that there exists a sequence σ'_d with $\pi(\sigma'_b) = \pi(\sigma'_c) + \pi(\sigma'_d)$ enabled at M'_d. In fact from eq. (1) it follows that

$$\begin{aligned} M'' &= M + C_u \cdot \pi(\sigma'_b) + C(\cdot, t) \\ &= M + C_u \cdot \pi(\sigma'_c) + C_u \cdot \pi(\sigma'_d) + C(\cdot, t) \end{aligned}$$

while from eq. (2) it follows that

$$M'_d = M + C_u \cdot \pi(\sigma'_c) + C(\cdot, t).$$

The last two equations imply that

$$M'' = M'_d + C_u \cdot \pi(\sigma'_d) \geq 0$$

and since the T_u-induced subnet is acyclic by Theorem 2.1 it holds that

$$M'_d[\sigma'_d\rangle M''. \tag{3}$$

Combining eqs. (1–3) we can write that

$$M_0[\sigma'_a\rangle M[\sigma'_c\rangle M'_c[t\rangle M'_d[\sigma'_d\rangle M''[\sigma''\rangle \tilde{M}.$$

This proves the result.

(If). If there exists a couple $(M, y) \in \mathcal{M}(w)$ *and a* $\sigma'' \in T_u^*$ *such that* $M[\sigma''\rangle \tilde{M}$ *and* $\tilde{y} = \pi(w) + y + \pi(\sigma'')$ *then* there exists $\sigma' \in T^*$ such that $M_0[\sigma'\rangle M[\sigma''\rangle \tilde{M}$ with $P_o(\sigma') = vt = w$ and hence $M_0[\sigma\rangle \tilde{M}$ with $\sigma = \sigma'\sigma''$.

Note that the *if* statement is true even if the unobservable subnet is not acyclic. □

Based on the above theorem we can prove that, for any $w \in T_o^*$ the set of consistent markings $\mathcal{C}(w)$ may be characterized in terms of a number of linear algebraic constraints. In particular, the number of constraints depends on the number of basis markings at w.

Corollary 3.9 *Let us consider a net system* $\langle N, M_0\rangle$ *whose unobservable subnet is acyclic. For any* $w \in T_o^*$ *it holds that* $\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid M = M_b + C_u \cdot y \ : \ y \geq \vec{0} \ \text{ and } \ M_b \in \mathcal{M}_{basis}(w)\}$.

Proof: Trivially follows from Theorems 2.1 and 3.8. □

The above result is particularly important in the case of bounded net systems because in such a case the number of constraints is finite for any observation w.

We conclude this section with an important result that is a key issue when performing diagnosis. Basically it consists in a restatement of Theorem 3.8 in terms of j-vectors.

Corollary 3.10 *Given a net system* $\langle N, M_0\rangle$ *where* $N = (P, T, Pre, Post)$ *and* $T = T_o \cup T_u$. *Assume that the* T_u*-induced subnet is acyclic. Let* $w = w't$ *be a given observation. The set* $Y_{\min}(M_0, w)$ *satisfies* $Y_{\min}(M_0, w) = \{y \in \mathbb{N}^{n_u} \mid y = y' + e : y' \in Y_{\min}(M_0, w'), e \in Y_{\min}(M'_b, t),\ M'_b = M_0 + C_u \cdot y' + C_o \cdot \pi(w')\}$.

Proof: It follows from Theorems 2.1, 3.8. In particular, a formal proof can be obtained by induction on the length of the observed string w, using the same arguments in the proof of Theorem 3.8.

□

In simple words, the set of j-vectors $Y_{\min}(M_0, w't)$ can be recursively computed from the j-vectors in $Y_{\min}(M_0, w')$ that lead to a basis marking M'_b that either enables t or enables a sequence of unobservable transitions enabling t.

Example 3.11 Let us consider the net system in Fig. 1. Let M_0 be the marking shown in the figure.

Let us consider the observation $w = t_1$. It holds that $\mathcal{J}(t_1) = \{\varepsilon\}$ and $Y_{\min}(M_0, t_1) = \{\vec{0}\}$, thus the basis marking associated to $w = t_1$ is $M_b = M_0 + C(\cdot, t_1) = [0\ 2\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$ and its j-vector is $\vec{0}$. Thus $\mathcal{M}(t_1) = \{(M_b, \vec{0})\}$.

Now, let us consider $w = t_1t_2$. In such a case the set of justifications are $\mathcal{J}(t_1t_2) = \{\varepsilon_3\varepsilon_4\varepsilon_5\varepsilon_6\varepsilon_7\varepsilon_8\varepsilon_9\varepsilon_{10}, \varepsilon_3\varepsilon_4\varepsilon_5$ $\varepsilon_6\varepsilon_3\varepsilon_{11}\varepsilon_8\varepsilon_9\varepsilon_{10}, \varepsilon_3\varepsilon_{11}\varepsilon_8\ \varepsilon_9\varepsilon_{10}\varepsilon_{13}\varepsilon_5\varepsilon_6, \varepsilon_7\varepsilon_8\varepsilon_9\varepsilon_{10}\varepsilon_{13}\varepsilon_5\varepsilon_6, \ldots\}$ where dots denote all other sequences (that have not been reported here for sake of conciseness) that are enabled at M_b and that have the same firing vector of the previous ones. The set of j-vectors is $Y_{\min}(M_b, t_2) = \{[1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0]^T,\ [2\,1\,1\,1\,0$ $1\ 1\ 0\ 0]^T,\ [1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1]^T, [0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1]^T\}$.

Now, let $e_1 = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0]^T, e_2 = [2\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0]^T, e_3 = [1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1]^T, e_4 = [0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1]^T\}$, the basis markings reached after the firing of w are:

$$\begin{aligned}
M_b^1 &= M_b + C_u \cdot e_1 + C(\cdot, t_2) = \\
&\quad [0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1]^T, \\
M_b^2 &= M_b + C_u \cdot e_2 + C(\cdot, t_2) = \\
&\quad [0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1]^T, \\
M_b^3 &= M_b + C_u \cdot e_3 + C(\cdot, t_2) = \\
&\quad [0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T, \\
M_b^4 &= M_b + C_u \cdot e_4 + C(\cdot, t_2) = \\
&\quad [0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T,
\end{aligned}$$

thus $\mathcal{M}(t_1t_2) = \{(M_b^1, e_1), (M_b^2, e_2), (M_b^3, e_3), (M_b^4, e_4)\}$ and $Y_{\min}(M_0, w) = Y_{\min}(M_b, t_2)$ being $Y_{\min}(M_0, t_1) = \{\vec{0}\}$. ■

4 Diagnosis states

Let us consider a system modeled as a Petri net whose transitions may either be observable or unobservable ($T = T_o \cup T_u$).

Assume that a certain number of *anomalous* (or *fault*) behaviors may occur in the system. The occurrence of a fault behavior corresponds to the firing of an unobservable transition, but there may also be other transitions that are unobservable as well, but whose firing corresponds to regular behaviors. Then, assume that fault behaviors may be divided into r main classes (*fault classes*), and we are not interested in distinguishing among fault events in the same class.

This can be easily modeled in PN terms assuming that the set of unobservable transitions is partitioned in two subsets, namely $T_u = T_f \cup T_{reg}$ where T_f includes all fault transitions and T_{reg} includes all transitions relative to unobservable but regular events. The set T_f is further partitioned in r subsets, namely, $T_f = T_f^1 \cup T_f^2 \cup \ldots \cup T_f^r$ where all transitions in the same subset correspond to the same fault class. We will say that the i-th fault has occurred when a transition in T_f^i has fired.

In the following subsection we introduce the definition of *diagnoser* and *diagnosis state*.

4.1 Basic definitions

Definition 4.1 A *diagnoser* is a function $\Delta : T_o^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{0, 1, 2, 3\}$ that associates to each observation w and to each fault class T_f^i, $i = 1, \ldots, r$, a *diagnosis state*.

• $\Delta(w, T_f^i) = 0$ if for all $\sigma \in \mathcal{L}(w)$ and for all $t_f \in T_f^i$ it holds that $t_f \notin \sigma$.

In such a case the ith fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions of class i.

• $\Delta(w, T_f^i) = 1$ if:
(i) there exist $\sigma \in \mathcal{L}(w)$ and $t_f \in T_f^i$ such that $t_f \in \sigma$ but
(ii) for all $\sigma \in \mathcal{J}(w)$ and for all $t_f \in T_f^i$ it holds that $t_f \notin \sigma$.

In such a case a fault transition of class i may have occurred but is not contained in any justification of w.

• $\Delta(w, T_f^i) = 2$ if there exist $\sigma, \sigma' \in \mathcal{J}(w)$ such that:
(i) there exists $t_f \in T_f^i$ such that $t_f \in \sigma$;
(ii) for all $t_f \in T_f^i$, $t_f \notin \sigma'$.

In such a case a fault transition of class i is contained in one (but not in all) justification of w.

• $\Delta(w, T_f^i) = 3$ if for all $\sigma \in \mathcal{L}(w)$ there exists $t_f \in T_f^i$ such that $t_f \in \sigma$.

In such a case the ith fault must have occurred, because all firable sequences consistent with the observation contain at least one fault transition of class i. ■

The diagnosis states 1 and 2 correspond both to cases in which a fault may have occurred but has not necessarily occurred. The main reason to distinguish between them is the following. In state 1 the observed behavior does not suggest that a fault has occurred because all minimal sequences leading to w are fault free. On the contrary, in state 2 at least one of the justifications of the observed behavior contains one transition in the class.

In practice diagnosis state 1 represents a situation that is common in many real applications. As an example, a break-down of a valve in a chemical plant may occur anytime thus all the states reached without a fault never fall into the diagnosis state 0 but in the diagnosis state 1.

Example 4.2 Consider the net system in Fig. 1. Assume that two different fault behaviors (fault classes) may occur: (1) either a plate is moved to the lower line or a slab is moved to the upper line ($T_f^1 = \{\varepsilon_{11}, \varepsilon_{12}\}$); (2) a plate of a different type (e.g., different material, or different size) enters the upper line ($T_f^2 = \{\varepsilon_{13}\}$).

Finally, let all the other unobservable transitions belong to set T_{reg}, this is $T_{reg} = \{\varepsilon_3, \varepsilon_4, \ldots, \varepsilon_{10}\}$.

Consider $\omega = \varepsilon$. It holds that $\mathcal{J}(\varepsilon) = \{\varepsilon\}$ and $\mathcal{L}(\varepsilon) = \{\varepsilon, \varepsilon_{13}, \varepsilon_{13}\varepsilon_5, \varepsilon_{13}\varepsilon_5\varepsilon_6\}$. Then, we may observe that transition $\varepsilon_{13} \in T_f^2$ may fire at M_0, while the other fault transitions are not enabled at M_0. Therefore, we conclude that $\Delta(\varepsilon, T_f^1) = 0$ and $\Delta(\varepsilon, T_f^2) = 1$.

Now, let us consider $\omega = t_1$. As already discussed in Example 3.11, one has $\mathcal{J}(t_1) = \{\varepsilon\}$ thus no fault transition may be contained in a justification of w. On the contrary, all fault transitions are contained in at least one sequence in $\mathcal{L}(t_1)$. Thus, $\Delta(t_1, T_f^1) = \Delta(t_1, T_f^2) = 1$.

Let us now focus on the observation $\omega = t_1t_2$. By looking at Example 3.11, it is easy to conclude that $\Delta(t_1t_2, T_f^1) = \Delta(t_1t_2, T_f^2) = 2$. In fact, all fault transitions are contained in at least one sequence in $\mathcal{J}(t_1t_2)$, but there are also justifications of t_1t_2 that do not contain fault transitions.

Finally, let $\omega = t_1t_2t_2$. In such a case one has $\Delta(\omega, T_f^1) = \Delta(\omega, T_f^2) = 3$ because as it can be easily verified, all justifications of w contain transitions of both classes. ■

The on-line computation of the sets $\mathcal{L}(w)$ and $\mathcal{J}(w)$ may be computational demanding in large scale systems, thus in the following we suggest two alternative procedures to compute diagnosis states. These procedures are based on the notions of *minimal explanations*, *minimal e-vectors*, and *basis markings*, that are presented in the following two sections. Both procedures apply to net systems whose *unobservable subnet is acyclic*, and the second one also requires that the net system is *bounded*.

4.2 Characterization of diagnosis states

In this subsection we provide some results that enable us to characterize the diagnosis states starting from the knowledge of the set $\mathcal{M}(w)$. The following two corollaries basically restate the definition of diagnosis states. In particular, the first one allows us to estimate the value of a diagnosis state, reached after the observation of a word w, from the analysis of the set $\mathcal{M}(w)$ defined in Definition 3.6.

Corollary 4.3 Consider an observed word $w \in T_o^*$.

• $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y) \in \mathcal{M}(w)$ and for all $t_f \in T_f^i$ it holds that $y(t_f) = 0$.

• $\Delta(w, T_f^i) = 2$ iff there exist $(M, y) \in \mathcal{M}(w)$ and $(M', y') \in \mathcal{M}(w)$ such that:
(i) there exists $t_f \in T_f^i$ such that $y(t_f) > 0$,
(ii) for all $t_f \in T_f^i$, $y'(t_f) = 0$.

• $\Delta(w, T_f^i) = 3$ iff for all $(M, y) \in \mathcal{M}(w)$ there exists $t_f \in T_f^i$ such that $y(t_f) > 0$.

The analysis of $\mathcal{M}(w)$ determines the states $\{0, 1\}$, 2 and 3, while to distinguish between states 0 and 1 further analysis is necessary. The following corollary shows how the states 0 and 1 can be distinguished with respect to the reachability of the unobservable net.

Corollary 4.4 Consider an observed word $w \in T_o^*$ such that $\forall (M, y) \in \mathcal{M}(w)$ and $\forall t_f \in T_f^i$ it holds that $y(t_f) = 0$.

• $\Delta(w, T_f^i) = 0$ if $\forall\ (M, y) \in \mathcal{M}(w)$ and $\forall t_f \in T_f^i$ there does not exist a sequence $\sigma \in T_u^*$ such that $M[\sigma\rangle$ and $t_f \in \sigma$.

• $\Delta(w, T_f^i) = 1$ if $\exists$ at least one $(M, y) \in \mathcal{M}(w)$ and a sequence $\sigma \in T_u^*$ such that for at least one $t_f \in T_f^i$, $M[\sigma\rangle$ and $t_f \in \sigma$.

The above result follows from the fact that by Corollary 4.3 $\Delta(w, T_f^i) \in \{0, 1\}$ if all the minimal justifications of w do not contain any fault transition of class i. However, by Definition 4.1, the diagnosis state is equal to zero if at each basis marking M at w no fault transition of class i is enabled. On the contrary the diagnosis state is equal to one if at least one fault transition of class i is enabled at one basis marking M at w.

If the *unobservable subnet is acyclic* the following proposition allows us to distinguish between the states 0 and 1 solving a trivial integer linear programming problem.

Proposition 4.5 For a PN whose unobservable subnet is acyclic, let $w \in T_o^*$ be an observed word such that for all $(M, y) \in \mathcal{M}(w)$ one has $y(t_f) = 0\ \forall\ t_f \in T_f^i$.

Let us consider the constraint set

$$\mathcal{T}_i(M) = \begin{cases} M + C_u \cdot z \geq \vec{0}, \\ \sum\limits_{t_f \in T_f^i} z(t_f) > 0, \\ z \in \mathbb{N}^{n_u}. \end{cases} \tag{4}$$

• $\Delta(w, T_f^i) = 0$ if $\forall\ (M, y) \in \mathcal{M}(w)$, $\mathcal{T}_i(M)$ is not feasible.

• $\Delta(w, T_f^i) = 1$ if $\exists\ (M, y) \in \mathcal{M}(w)$ such that $\mathcal{T}_i(M)$ is feasible.

Proof: Follows from Corollary 4.4 and the fact that, by Theorem 2.1, if the unobservable subnet is acyclic, $\mathcal{T}_i(M)$ characterizes the reachability set of the unobservable net. Thus, there exists a sequence containing a transition $t_f \in T_f^i$ firable at M on the unobservable subnet if and only if

$\mathcal{T}_i(M)$ is feasible. □

Example 4.6 Consider again the net system in Fig. 1. Let $w = \varepsilon$. It holds that $\mathcal{M}(\varepsilon) = \{(M_0, \vec{0})\}$, thus by Corollary 4.3, $\Delta(\varepsilon, T_f^1) = \Delta(\varepsilon, T_f^2) \in \{0, 1\}$. To completely determine the diagnosis states we need to verify if the integer constraint sets defined in Proposition 4.5 admit solutions. This is not true in the case of the first class, while it is the case for the second class. Therefore we conclude that $\Delta(\varepsilon, T_f^1) = 0$ and $\Delta(\varepsilon, T_f^2) = 1$, that is in accordance with Example 4.2. ■

5 Diagnosis of bounded systems

In this section we focus on *bounded* PNs and we show how in such a case the most burdersome part of the procedure can be moved off-line. In particular, we present an original technique to design an observer to be used for on-line diagnosis.

5.1 Basis reachability graph

The proposed observer is based on the construction of a deterministic graph, that we call *basis reachability graph* (BRG). As discussed later, the main advantage of using BRG is that it enables us to move off-line most of the computations.

Definition 5.1 *The BRG is a deterministic graph that has as many nodes as the number of possible basis markings.*

To each node is associated a different basis marking and a row vector with as many entries as the number of fault classes. The entries of this vector may only take binary values: 1 if $\mathcal{T}_i(M)$ is feasible for M equal to the basis marking, 0 otherwise.

Arcs are labeled with observable transitions and e-vectors. More precisely, an arc exists from node containing the basis marking M to node containing the basis marking M' if and only if there exists an observable transition t for which an explanation exists at M and the firing of t and one of its minimal explanations leads to M'. The arc going from M to M' is labeled (t, e), where $e \in Y_{\min}(M, t)$ and $M' = M + C_u \cdot e + C(\cdot, t)$. ■

Note that the number of nodes of the BRG is always finite since the net system is bounded. Moreover, the row vector of binary values associated to the nodes of the BRG allows us to distinguish between the diagnosis state 1 or 0.

The following algorithm provides a systematic procedure to compute the BRG.

Algorithm 5.2 [Computation of the BRG]

Input: a net system $\langle N, M_0 \rangle$,
the set of unobservable transitions T_u,

M_0	[	1	0	0	0	0	0	0	0	0	0	0	1	1	$]^T$
M_1	[	0	2	0	0	0	0	1	0	0	0	0	1	1	$]^T$
M_2	[	0	1	0	0	0	0	0	0	0	0	1	1	1	$]^T$
M_3	[	0	0	0	0	0	0	1	0	0	0	0	1	0	1	$]^T$
M_4	[	0	1	0	0	0	0	1	0	0	0	0	1	0	0	$]^T$
M_5	[	0	2	0	0	0	0	0	0	0	0	0	1	1	0	$]^T$
M_6	[	0	0	0	0	0	0	0	0	0	0	0	2	0	0	$]^T$

Table 1: The basis markings of the BRG in Fig. 2.

the fault classes $\{T_f^i\}_{i=1,\ldots,r}$.

Output: the BRG.

1. Label the initial node (M_0, x_0) with $\forall i \in \{1, \ldots, r\}$,

$$x_0(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}_i(M_0) \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$$

No tag is assigned to it.

2. While nodes with no tag exist

select a node with no tag and do

2.1. let M be the marking in the node,

2.2. for all t such that $Y_{\min}(M, t) \neq \emptyset$, do

2.2.1. for all $e \in Y_{\min}(M, t)$, do

2.2.1.1. let $M' = M + C_u \cdot e + C(\cdot, t)$,

2.2.1.2. if $\nexists$ a node with M', then

add a new node labeled (M', x')

with $\forall i \in \{1, \ldots, r\}$,

$$x'(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}_i(M') \text{ is feasible,} \\ 0 & \text{otherwise,} \end{cases}$$

2.3. tag the node "old".

3. Remove all tags. ■

The algorithm constructs the BRG starting from the initial node that is labeled by a pair (M_0, x_0) where M_0 is the initial marking and x_0 is a binary row vector that specifies for each fault class if a fault in that class may occur by firing only unobservable transitions. Now, we consider all observable transitions for which a minimal explanation at M_0 exists. For any of these transitions $t \in T_o$ we compute the marking resulting from firing t at $M_0 + C_u \cdot e$, for each $e \in Y_{\min}(M_0, t)$. If a marking not contained in the previous nodes is obtained, a new node is added to the graph. The arc going from the initial node to the new node is labeled (t, e). The procedure is iterated until all basis markings have been considered.

Example 5.3 In Fig. 2 we have reported the BRG of the net system in Fig.1. The notation used in Fig. 2 is detailed in Tables 1 and 2. Each node of the graph contains a different basis marking and a row vector that has two entries as the number of fault classes. As an example, the vector [0 1] is associated to M_0 because the constraint set $\mathcal{T}_i(M_0)$ is not feasible for $i = 1$, while it is

	ε_3	ε_4	ε_5	ε_6	ε_7	ε_8	ε_9	ε_{10}	ε_{11}	ε_{12}	ε_{13}
e_1	1	1	1	1	1	1	1	1	0	0	0
e_2	2	1	1	1	0	1	1	1	1	0	0
e_3	1	0	1	1	0	1	1	1	1	0	1
e_4	0	0	1	1	1	1	1	1	0	0	1

Table 2: The e-vectors of the BRG in Fig. 2

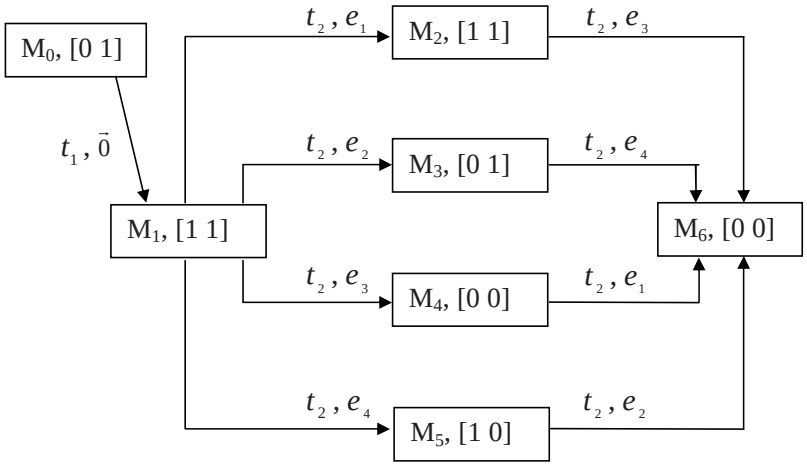

Figure 2: The BRG of the net in Fig. 1.

feasible for $i = 2$. Then, there is an arc labeled $(t_1, \vec{0})$ from M_0 to M_1 because t_1 is enabled at M_0 and its firing leads to M_1. Note that in such a case $Y_{\min}(M_0, t_1) = \{\vec{0}\}$. Furthermore, there are four arcs exiting from node M_1, all labeled t_2 and containing minimal explanations e_1, e_2, e_3 and e_4, respectively, and leading to nodes containing markings M_2, M_3, M_4 and M_5, respectively.

Note that, by looking at the BRG we can also read all sequences of observable words, that is finite in the case at hand, and equal to $\{\varepsilon, t_1, t_1t_2, t_1t_2t_2\}$. Moreover note that for all the j-vectors in Table 2 the component associated to ε_{12} is equal to 0. This means that ε_{12} can never be detected. ■

5.2 On-line diagnosis using BRG

The following algorithm summarizes the main steps to compute the diagnosis states by looking at the BRG.

Algorithm 5.4 [Diagnosis using the BRG]

Input: a net system $\langle N, M_0 \rangle$,
the set of unobservable transitions T_u,
the fault classes $\{T_f^i\}_{i=1,\ldots,r}$.
the BRG.

Output: the diagnosis states.

1. Let $w = \varepsilon$.

2. Let $\mathcal{M}(w) = \{(M_0, \vec{0})\}$.

3. Wait until a new transition t fires.

4. Let $w' = w$ and $w = w't$.

5. Let $\mathcal{M}(w) = \emptyset$, **[Comp. of $\mathcal{M}(w)$]**

6. For all couples $(M', y') \in \mathcal{M}(w')$, do

6.1. for all arcs exiting from node (M', x')
in the BRG and labeled (t, e), do

6.1.1. let $M = M' + C_u \cdot e + C(\cdot, t)$,

6.1.2. let $y = y' + e$,

6.1.3. let $\mathcal{M}(w) = \mathcal{M}(w) \cup \{(M, y)\}$.

7. For all $i \in \{1, \ldots, r\}$, do **[Comp. diag. state]**

7.1. if $\forall\ (M, y) \in \mathcal{M}(w)$ and $\forall t_f \in T_f^i$
it holds $y(t_f) = 0$, then
if $\forall\ (M, y) \in \mathcal{M}(w)$ it holds that $x(i) = 0$,
where x is the binary vector
in the node M of the BRG, then
let $\Delta(w, T_f^i) = 0$,
else
let $\Delta(w, T_f^i) = 1$,

7.2. if $\exists\ (M, y) \in \mathcal{M}(w)$ and $\exists (M', y') \in \mathcal{M}(w)$
such that:
(i) $\exists t_f \in T_f^i$ such that $y(t_f) > 0$,
(ii) $\forall t_f \in T_f^i$, $y'(t_f) = 0$, then
let $\Delta(w, T_f^i) = 2$,

7.3. if $\forall\ (M, y) \in \mathcal{M}(w)\ \exists t_f \in T_f^i$
such that $y(t_f) > 0$, then
let $\Delta(w, T_f^i) = 3$.

8. Goto step 3. ■

Steps 1 to 6 of Algorithm 5.4 compute the set $\mathcal{M}(w)$. When no event is observed, namely $w = \varepsilon$, then $\mathcal{M}(w) = \{(M_0, \vec{0})\}$. Now, assume that a transition t is observed. We include in the set $\mathcal{M}(t)$ all couples (M, y) such that an arc labeled t exits from the initial node and ends in a node containing the basis marking M. The corresponding value of y is equal to the e-vector in the arc going from M_0 to M, being $\vec{0}$ the j-vector relative to M_0. In general, if w' is the actual observation, and a new transition t fires, we consider all couples $(M', y') \in \mathcal{M}(w')$ and all nodes that can be reached from M' with an arc labeled t. Let M be the basis marking of the generic resulting node. We include in $\mathcal{M}(w) = \mathcal{M}(w't)$ all couples (M, y), where for any M, y is equal to the sum of y' plus the e-vector labeling the arc from M' to M.

Step 7 of Algorithm 5.4 computes the diagnosis state. Let us consider the generic ith fault class. If $\forall (M, y) \in \mathcal{M}(w)$ and $\forall t_f \in T_f^i$ it holds that $y(t_f) = 0$, we have to check the ith entry of all the binary row vectors associated to the basis markings M, such that $(M, y) \in \mathcal{M}(w)$. If these entries are all equal to 0, we set $\Delta(w, T_f^i) = 0$, otherwise we set $\Delta(w, T_f^i) = 1$. On the other

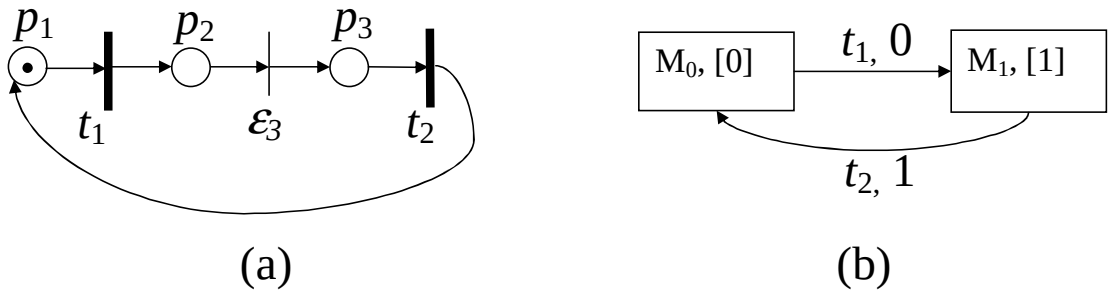

Figure 3: The PN of the Example 5.6 (a) and its BRG (b).

hand, if there exists at least one pair $(M, y) \in \mathcal{M}(w)$ with $y(t_f) > 0$ for any $t_f \in T_f^i$, and there exists at least one pair $(M', y') \in \mathcal{M}(w)$ with $y(t_f) = 0$ for all $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 2$. Finally, if for all pairs $(M, y) \in \mathcal{M}(w)$ $y(t_f) > 0$ for any $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 3$.

Example 5.5 Consider the BRG in Fig. 2 relative to the net system in Fig. 1, where $T_f^1 = \{\varepsilon_{11}, \varepsilon_{12}\}$ and $T_f^2 = \{\varepsilon_{13}\}$. Let $w = \varepsilon$. By looking at the BRG we establish that $\Delta(\varepsilon, T_f^1) = 0$ and $\Delta(\varepsilon, T_f^2) = 1$, because the first entry of the row vector in the node M_0 is 0, while its second entry is equal to 1.

Now, let $w = t_1 t_2$. In such a case $\mathcal{M}(w) = \{(M_2, y_1),\ (M_3, y_2), (M_4, y_3), (M_5, y_4)\}$, where $y_1 = \vec{0} + e_1 = e_1$, $y_2 = \vec{0} + e_2 = e_2$, $y_3 = \vec{0} + e_3 = e_3$, $y_4 = \vec{0} + e_4 = e_4$.

It holds that $\Delta(t_1 t_2, T_f^1) = 2$ being $y_2(\varepsilon_{11}) = y_3(\varepsilon_{11}) = 1$ and $y_1(\varepsilon_{11}) = y_4(\varepsilon_{11}) = y_j(\varepsilon_{12}) = 0$ for $j = 1, 4$. Analogously, $\Delta(t_1 t_2, T_f^2) = 2$ being $y_3(\varepsilon_{13}) = y_4(\varepsilon_{13}) = 1$ and $y_1(\varepsilon_{13}) = y_2(\varepsilon_{13}) = 0$.

Finally, for $w = t_1 t_2 t_2$ one has $\Delta(t_1 t_2 t_2, T_f^i) = 3$ for $i = 1, 2$. In fact $\mathcal{M}(w) = \{(M_6, y_5), (M_6, y_6)\}$, where $y_5 = y_1 + e_3 = y_3 + e_1$, $y_6 = y_2 + e_4 = y_4 + e_2$, and $y_5(\varepsilon_{11}) = y_6(\varepsilon_{11}) = 1$, $y_5(\varepsilon_{13}) = y_6(\varepsilon_{13}) = 1$. ■

In the previous example we considered a net that does not contain repetitive sequences and the corresponding BRG is acyclic. In such a case, we could also determine off-line the j-vector associated to each basis marking. However, our procedure applies to the more general case of bounded PNs with repetitive sequences, to which a cyclic BRG corresponds. For this class of nets we need to compute the j-vector of a basis marking on-line as shown in the following example.

Example 5.6 Consider the bounded PN shown in Fig. 3(a), where $T_o = \{t_1, t_2\}$ and $T_u = \{\varepsilon_3\}$. We assume that the only fault that can occur is $T_1^f = \{\varepsilon_3\}$. This net contains the repetitive sequence $t_1 \varepsilon_3 t_2$ that can fire infinitely often, hence its BRG is cyclic as shown in Fig. 5.6(b), where the basis markings are $M_0 = [1\ 0\ 0]^T$ and $M_1 = [0\ 1\ 0]^T$.

It is easy to verify that in this case we cannot associate off-line j-vectors to basis markings. In fact when $w = \varepsilon$ the j-vector associated to node $M_0, [0]$ is $[0]$, hence the diagnosis state is $\Delta(\varepsilon, T_1^f) = 0$. On the contrary, after $w = t_1 t_2$ fires we reach the same basis marking $M_0, [0]$ but now its j-vector is $[1]$, and the diagnosis state is changed to $\Delta(t_1 t_2, T_1^f) = 3$. ■

6 Conclusions and future work

In this paper we presented an approach for the on-line diagnosis of discrete event systems using PNs. Faults are modeled as unobservable transitions, and legal behaviors as well may be modeled as unobservable transitions. Different diagnosis states are defined, that correspond to different degrees of alarm. Their computation are based on the notions of basis markings and j-vectors. The advantage of our approach is even more evident in the case of bounded Petri nets. Indeed in such a case, the most burdensome part of the procedure may be moved off-line thanks to the definition of the *basis reachability graph*.

Note that the proposed results have several implications, not only related to diagnosis. In particular, they may be useful when controlling a system with unobservable (or silent) events.

Our future work in this topic will follow several directions. Firstly, we want to extend the proposed procedure to labeled PNs. In such a case a further form of nondeterminism should be taken into account because two or more transitions may share the same label. Then, we would like to extend the definition of basis reachability graph to unbounded net systems. Finally, we plan to provide necessary and sufficient conditions for a language to be diagnosable.

References

[1] F. Basile, P. Chiacchio, and G. De Tommasi. An efficient approach for online diagnosis of discrete event systems. *IEEE Trans. Automatic Control*, 54(4):748–759, 2009.

[2] A. Benveniste, E. Fabre, S. Haar, and C. Jard. Diagnosis of asynchronous discrete event systems: A net unfolding approach. *IEEE Trans. Automatic Control*, 48(5):714–727, 2003.

[3] R.K. Boel and G. Jiroveanu. Distributed contextual diagnosis for very large systems. In *Proc. IFAC WODES'04: 7th Work. on Discrete Event Systems (Reims, France)*, pages 343–348, September 2004.

[4] R.K. Boel and J.H. van Schuppen. Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers. In *Proc. WODES'02: 6th Work. on Discrete Event Systems (Zaragoza, Spain)*, pages 175–181, October 2002.

[5] M.P. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Technical Report at: http://www.diee.unica.it/∼seatzu/TRcabasino.pdf*, 2009.

[6] D. Corona, A. Giua, and C. Seatzu. Marking estimation of Petri nets with silent transitions. *IEEE Trans. Automatic Control*, 52(9):1695–1699, September 2007.

[7] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete-event systems. *Discrete Event Dynamical Systems*, 10(1):33–86, January 2000.

[8] M. Dotoli, M.P. Fanti, and A.M. Mangini. Fault detection of discrete event systems using Petri nets and integer linear programming. In *Proc. of 17th IFAC World Congress*, Seoul, Korea, July 2008.

[9] S. Genc and S. Lafortune. Distributed diagnosis of place-bordered Petri nets. *IEEE Trans. on Automation Science and Engineering*, 4(2):206–219, 2007.

[10] A. Giua and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. In *Proc. 44th IEEE Conf. on Decision and Control*, pages 6323–6328, December 2005.

[11] G. Jiroveanu and R.K. Boel. Contextual analysis of Petri nets for distributed applications. In *16th Int. Symp. on Mathematical Theory of Networks and Systems (Leuven, Belgium)*, July 2004.

[12] J. Martinez and M. Silva. A simple and fast algorithm to obtain all invariants of a generalized Petri net. In Girault, C. and Reisig, W., editors, *Informatik-Fachberichte 52: Application and Theory of Petri Nets*.

[13] J. Prock. A new technique for fault detection using Petri nets. *Automatica*, 27(2):239–245, 1991.

[14] M. Sampath, S. Lafortune, and D. Teneketzis. Active diagnosis of discrete-event systems. *IEEE Trans. Automatic Control*, 43(7):908–929, July 1998.

[15] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Trans. Automatic Control*, 40 (9):1555–1575, 1995.

[16] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Failure diagnosis using discrete-event models. *IEEE Trans. Control Systems Technology*, 4(2):105–124, 1996.

[17] S. Hashtrudi Zad, R.H. Kwong, and W.M. Wonham. Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Trans. Automatic Control*, 48(7):1199–1212, July 2003.